UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/677,660	10/02/2003	**Susann Marie Keohane**	AUS920030640US1	9966

60501 7590 03/18/2009

LENOVO COMPANY
c/o BIGGERS & OHANIAN, LLP
P.O. BOX 1469
AUSTIN, TX 78767-1469

EXAMINER	
PHAN, TUANKHANH D	
ART UNIT	**PAPER NUMBER**
2163	
MAIL DATE	**DELIVERY MODE**
03/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/677,660
Filing Date: October 02, 2003
Appellant(s): KEOHANE ET AL.

Brandon C. Kennedy
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/05/2008 appealing from the Office action mailed 07/17/2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

The following are the evidences relied upon in the rejection of claims under appeal:

Herrero et al. WO 2000/74345. Date of Publication: Dec. 07, 2000.

Holden et al. US Patent No. 5,828,832. Date of Patent: Oct. 27, 1998.

Ueda et al. US Patent No. 5,692,179. Date of Patent: Nov. 25, 1997.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herrero et al. (WO 00/74345), hereinafter Herrero, in view of Holden et al. (US Pat. 5,828,832), hereinafter Holden.

Regarding claims 1, 14 and 27, Herrero discloses a method/system for providing a necessary level of security for a computer capable of connecting to different computing environments are determined (i.e. **providing security requirements for**

establishment between entities in one or more networks and determining the needed security levels for data and connections, abstract), the method comprising:

monitoring a type of connection between the computer and a network in a current computing environment (i.e. **measuring security for connection exist between entities – e.g. a computer and its network,** p. 4 lines 5-10);

determining a security level of data before sending the data across the network (i.e. **determine the security level needed based on the information, data, being transmitted,** p. 4, lines 13-14);

but Herrero does not explicitly teach storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and sending the data from the buffer.

However, in the same field of endeavor, Holden discloses storing the data in a buffer (i.e. **storing the datagram/data, in the waiting queue/buffer, col. 11, lines 28-30**), instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data (i.e. **then waiting to be sent across the network upon exchanged and met security requirements – association grant message received, col. 11, lines 30-31**); and

Holden discloses sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (i.e. **upon the verification of**

connection/receiver and security control required for the datagram is validated, datagram is sent from the queue/buffer, col. 11, lines 50-52).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the waiting buffer for data security taught by Holden into the verification of connection security taught by Herrero to allow the operations of computer network entities transmitting secured data across the network with out any expensive network security interfaces (Holden).

Regarding claims 2, 15 and 28, Herrero and Holden disclose the method of claims 1, 14 and 27, and Holden further discloses wherein monitoring a type of connection comprises periodically determining the type of connection between the computer and the network (i.e. the procedure of checking destination network connection is repeated/periodically, col. 19, lines 13-14).

Regarding claims 3, 16 and 29, Herrero and Holden disclose the method of claims 1, 14 and 27, Holden further discloses wherein monitoring a type of connection comprises event-driven determining of the type of connection between the computer and the network (i.e. **processing based on an anticipated event is equivalent to event-driven determination**, col. 16, lines 56-57).

Regarding claims 4, 17 and 30, Herrero and Holden disclose the method of claims 3, 16 and 29, Holden further discloses wherein the steps of the method are carried out by a software process and event-driven determining of the type of connection is carried out whenever the process is invoked (col. 16, lines 56-57).

Regarding claims 5, 18 and 31, Herrero and Holden disclose the method of claims 3, 16 and 29, wherein determining a security level results in a determination that data to be transmitted requires at least some level of security and event-driven determining of the type of connection is carried out in response to such determination (see the discussions of level of security of data in claim 1 and event-driven in claim 3).

Regarding claims 6, 19 and 32, Herrero and Holden disclose the method of claims 1, 14 and 27, Herrero further discloses wherein determining a security level of data before sending the data across the current network comprises reading the security level of data from a markup element embedded in the data (i.e. markup element embedded in the data is a form of applying data encryption or data masking, p. 6, lines 15-17).

Regarding claims 7, 20 and 33, Herrero and Holden disclose the method of claims 1, 14 and 27, Holden further discloses wherein determining a security level of data before sending the data across the current network comprises reading the security level of data from meta-data in a header in a network message (IP datagrams, e.g. IP header, is a type of meta-data, col. 16, line 56).

Regarding claims 8, 21 and 34, Herrero and Holden disclose the method of claims 1, 14 and 27, Herrero further discloses comprising returning a non-fatal error to a sending program if the connection to the network lacks a security control required for the data (enable looping, Figure 7, allows a future or alternative checking such that non-fatal error is considered).

Regarding claims 9, 22 and 35, Herrero and Holden disclose the method of claims 8, 21 and 34, Holden discloses further comprising the sending program's informing a user that the data will be held in a security buffer until the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (i.e. **storing the datagram/data, in the waiting queue/buffer, col. 11, lines 28-30, then waiting to be sent across the network upon exchanged and met security requirements – association grant message received, col. 11, lines 30-31**).

Regarding claims 10, 23 and 36, Herrero and Holden disclose the method of claims 8, 21 and 34, Herrero discloses further comprising the sending program's prompting a user with the option to create a secure tunnel for transmission of the data (security level needed may be determined, p. 4, lines 10-13).

Regarding claims 11, 24 and 37, see discussion of claims 1 above, Herrero further discloses a method for providing a necessary level of security for a computer capable of connecting to different computing environments, the method comprising:

connecting the computer to a network in a first computing environment determined (i.e. **providing security requirements for establishment between entities in one or more networks and determining the needed security levels for data and connections**, abstract);

specifying a security level for data to be sent across the network (abstract);

instructing a sending program to send the data across the network (abstract);

receiving an indication that security control of the first computing environment lacks a security control required for the specified security level (p. 4, lines 5-20);

connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level (p. 4, lines 5-20); and

receiving an indication that the data has been sent across the network (p. 10, lines 25).

Regarding claims 12, 25 and 38, Herrero and Holden disclose the method of claims 11, 24 and 37, Herrero further discloses comprising: determining, when the computer is connected to the second network, that the second computing environment has the security control required for the specified security level (i.e. **providing security requirements for establishment between entities in one or more networks and determining the needed security levels for data and connections**, abstract); and

automatically sending the data across the network promptly upon determining that the second computing environment has the security control required for the specified security level (abstract).

Regarding claims 13, 26 and 39, Herrero and Holden disclose the method of claims 11, 24 and 37, Herrero further discloses comprising: receiving an indication that the second computing environment has the security control required for the specified security level (p. 4); and again instructing the sending program to send the data across the network (Figure 7, "770").

Claims 1, 14 and 27 are also rejected **under 35 U.S.C. 103(a)** as being unpatentable over Herrero et al. (WO 00/74345), hereinafter Herrero, in view of Ueda (US Pat. 5,692,179).

Regarding claims 1, 14 and 27, Herrero discloses a method/system for providing a necessary level of security for a computer capable of connecting to different computing environments are determined (i.e. **providing security requirements for establishment between entities in one or more networks and determining the needed security levels for data and connections**, abstract), the method comprising:

monitoring a type of connection between the computer and a network in a current computing environment (i.e. **measuring security for connection exist between entities – e.g. a computer and its network,** p. 4 lines 5-10);

determining a security level of data before sending the data across the network (i.e. **determine the security level needed based on the information, data, being transmitted,** p. 4, lines 13-14);

but Herrero does not explicitly teach storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data; and sending the data from the buffer.

However, in the same field of endeavor, Ueda discloses storing the data in a buffer (i.e**. data are temporarily stored to the buffer means**, col. 4, lines 60-62) instead of sending the data across the network if the connection to the network lacks a

security control required for the determined security level of the data (col. 4, lines 60-62); and

Ueda discloses sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data (i.e. **and then transmitted when security level of the connection and security level of data are in conformity**, col. 4, lines 59-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the waiting buffer for data security taught by Ueda into the connection security taught by Herrero to allow the operations of computer network entities transmitting secured data across the network instantly upon registration of security network by another user (Ueda).

(10) Response to Argument

I (Issue): Do Herrero et al. in view of Holden et al. show or suggest "*storing the data in a buffer of sending the data from the buffer*" in combination with the features as is required by claim 1 of the present application?

- In the first argument, the Appellants argue that *Holden discloses a 'Waiting Queue' used by a serial network interface unit ('SNIU') to store user-data grams until an association is established between the SNIU and the destination user through an exchange of association request and grant messages. Holden's "Waiting Queue,' however, does not disclose the buffer as claimed in the present application because the buffer as claimed in the present application effectively stores data until a computer's network connection is changed from a connection*

lacking the required security control to a connection having the required security control. Holden only discloses holding data until establishing an association with a destination user - not sending data upon a change from a network connection lacking the required security control to a connection having the required security control as claimed here. In fact, Holden is not concerned with, and therefore does not disclose, a changed computing environment having a new type of connection as claimed in the present invention. Holden therefore neither discloses nor suggests storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data and sending the data from the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data as claimed here.

In response to the first argument, the Appellants' argument has not been found to be persuasive. In fact the Appellants seem to agree with the disclosures of Holden et al. where having a Waiting Queue stored data (col. 11, lines 28-29; i.e. data being stored in the buffer queue) until the network connection is secured (col. 11, lines 30-31; i.e. the security of network connection is checked and grant up on receiving a confirmed message), then data is sent out from the waiting Queue to the destination (col. 11, line 33; data being encrypted and sent). In addition, it is well known in the art that a waiting queue or a waiting buffer queue is no difference than the "buffer" of the claimed invention. Thus, Appellants' arguments of dependent claims 2-10 are found not to be persuasive.

II (Issue): Do Herrero et al. show or suggest connecting the computer the network in a second computing environment?

- In the second argument, the Appellants argue that *Herrero only discloses secure communications through use of security bindings between entities on a network - not by connecting a computer to a second computing environment. In fact, Herrero never once discloses, mentions, or even contemplates providing a necessary level of security for a computer by connecting the computer to a second computing environment as claimed here, that is, by changing the connection between a computer and a network from a first computing environment to a second computing environment. As such, Herrero does not disclose or suggest connecting the computer to the network in a second computing environment, wherein the second computing environment has the security control required for the specified security level as claimed in the present application.*

In response to the second argument, the Appellants' argument has not been found to be persuasive. The Examiner respectfully disagrees with the Appellants, for Herrero et al. clearly disclose connecting to a second computing environment with different entities (page 4, lines 5-20; i.e. network establishment between entities in one or more networks based on the requirement). In addition, Herrero et al. disclose at least two different computing environments for connections (page 2, lines 20-22; i.e. a Home PLMN and Visitor PLMN environments). Thus, Appellants' arguments of dependent claims 12-13 are found not to be persuasive.

Because the combination of Herrero et al. in view of Holden et al. disclose each and every element of independent claims 11, 11, 14, 24, 27 and 37 is valid, claims 1-39 stand rejected.

III (Issue): Do Herrero et al. in view of Ueda et al. show or suggest "*storing the data in a buffer of sending the data from the buffer*" in combination with the features as is required by claims 1, 14 and 27 of the present application?

- In the third argument, the Appellants argue that *Ueda's temporary storage of data in a buffer and transmission of the data from the buffer does not disclose storing data in a buffer and sending the data from the buffer when a computer is connected to a changed computing environment having a new type of connection as claimed in the present application. Ueda at most discloses a well known method of data communications, used in many standard data communications protocols, in which data is stored in a buffer prior to transmission across a network. In many implementations of the common TCP/IP data communications protocol, data is stored in a buffer prior to being packetized for transmission across a network. Ueda does not disclose, however, storing data in a buffer on a computer until the computer's network connection is changed to one having a security control required for the data, evidenced by the fact that Ueda is only concerned with the security level of an inquirer, a user, a person, with respect to requested data, not the security level of a network connection. Ueda therefore neither discloses nor suggests storing the data in a buffer instead of sending the data across the network if the connection to the network lacks a security control required for the determined security level of the data and sending the data from*

the buffer when the computer is connected to a changed computing environment having a new type of connection that has the security control required for the data as claimed here.

In response to the third argument, the Appellants' argument has not been found to be persuasive. The Examiner respectfully disagrees with the Appellants because Ueda discloses determination of network control and management upon checking the network retrieving situation from on terminal via signal transmitting through the network – that is the predetermined condition of the network (col. 5, lines 52-56), and if the condition of the network is not satisfied, data is being stored by an inputting buffer means (col. 5, lines 48-50).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Information Disclosure Statement, filed 2/17/2009, has not been considered.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Tuankhanh Phan

Conferees:

A. Don Wong, SPE AU 2163

/don wong/

Supervisory Patent Examiner, Art Unit 2163

/John Breene/

Supervisory Patent Examiner, Art Unit 2162

C. TuanKhanh Phan, Examiner AU 2163